L.G.S. Master Copy

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C 20301-3040

COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF.
DIRECTORS OF DEFENSE AGENCIES

SUBJECT: Automated Message Processing

In a 1 February 1979 memorandum, ASD(C^3I) promulgated the DoD plan for automated message handling systems. The plan included tasking to DCA to develop an Integrated AUTODIN System Architecture (IASA) and to develop the Inter-Service/Agency AMPE (I-S/A AMPE). The plan further tasked DIA to provide a communication support processor (CSP) to meet near term service/agency special security office automation needs. In a 9 June 1980 memorandum, ASD(C^3I) approved the IASA Report (Part 2) which included specific implementation details and scope for I-S/A AMPE. In the approval memorandum all near-term implementations of new or upgraded AMPE sites were subject to review and approval by ASD(C^3I). Proposed procurements of all non-AMPE telecommunications terminals which interface the DCS or interconnect via the AUTODIN backbone were also subject to review and approval by ASD(C^3I) after being submitted through DCA.

The major near-term communications systems which will be transitioned to I-S/A AMPE and which are subject to the provisions of the 9 June 1980 memorandum include: Automated Multi-media Exchange (AMME); Local Digital Message Exchange (LDMX); STREAMLINER; Communications Support Processor (CSP); and Air Force AMPE (AF AMPE). Replacement of Air Force RAIDs and exportation of the Army PACS are also subject to these provisions. All requirements to place these systems in new locations or to upgrade an existing system must be reviewed by this office and will be approved only on an urgent mission requirement basis.

Request the Director, DCA, in conjunction with the Air Force as the Lead Military Department, and the responsible Service or Agency, insure that each of the above systems is reviewed promptly for inclusion in the planning and scheduling for transition to I-S/A AMPE. This review, especially for the CSP, should examine the current costs and functionality of the system in comparison to the projected costs and functionality of I-S/A AMPE.

THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

28 JAN 1985

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Automated Information Systems Security

I have reviewed the report prepared by Director, National Security Agency (DIRNSA), in coordination with Under Secretary of Defense for Research and Engineering (USDRE) and Under Secretary of Defense for Policy (USD(P)), that resulted from the examination of the policies, organizational arrangements, and programmatic aspects involved in automated information systems security. This examination was directed by my 12 January 1984 memorandum, same subject as above. As a result of my review of the report, I direct that the following actions be initiated:

(a) The USD(P) will:

(1) in collaboration with the Computer Security Evaluation Center, prepare a revised DODD 5200.28 which will expand the scope of the present directive to include all computer-driven information systems and which will provide expanded policy guidance on mandatory statements of computer security requirements for all ADP procurements and the use of computer security guidelines and standards.

(2) upon issuance of the Trusted Computer System Evaluation Criteria, revise DODD 5200.28 and 5100.55 to encourage system managers for US networks that interoperate with the systems of our allies to ensure that all components are evaluated by a common security criteria.

(b) The DIRNSA will:

(1) establish an ad hoc working group to develop a common set of security criteria for use by all Designated Approving Authorities.

(2) develop a Computer Security Vulnerability Reporting Program.

01433

Next 1 Page(s) In Document Denied

Approved For Release 2009/06/30 : CIA-RDP89B01354R000100170030-0

SECRET

The Director of Central Intelligence

Washington D C 20505

NFIC-9.11/1
22 January 1985

MEMORANDUM FOR: See Distribution

SUBJECT: Reports on Computer Security for SCI-Handling Systems

1. The DCI's Computer Security (COMPUSEC) Project began in April 1983 and is intended to support the DCI in assessing the security of automated systems processing information derived from sensitive methods and sources, to identify the threats to automated systems processing such materials, and to recommend actions for the DCI that will allow him to attest to the acceptability of operating risks. 25X1

2. As part of the DCI's COMPUSEC Project, the COMPUSEC Project Team developed an assessment on the threat to US automated Intelligence Community systems (See Attachment 1). Representatives from the NFIC Community have provided input to this document. This formulation of the "threat" is being used in conjunction with security assessments of the Intelligence Community's "critical" automated SCI systems to set program and budget priorities for immediate security upgrades. This threat point paper also serves to fulfill one of the DCI's continuing distinctive responsibilities. 25X1

3. The SAFEGUARDS document (Attachment 2) identifies security requirements for the protection of SCI information in the "critical" systems evaluated as part of the DCI's Computer Security (COMPUSEC) Project. When fully implemented in the "critical" systems, the SAFEGUARDS will correct the security shortfalls and reduce to an acceptable level the risks currently associated with processing this sensitive information in the "critical" systems. I intend to direct that the SAFEGUARDS be imposed as mandatory standards for the 13 "critical" SCI-handling systems by the end of FY 86. These SAFEGUARDS will also be imposed as voluntary standards for other SCI-handling systems. 25X1

4. In June 1984, an interagency Computer Security Technology Panel was established to assess the application of computer security technologies against known operational deficiencies within Intelligence Community computer systems. The panel focused on what could be done, in the near term, with existing computer security technology and administrative/management actions to provide security upgrades for our "critical" systems. Specific emphasis was given to three areas of computer security vulnerability: authentication of

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

CL BY SIGNER
DECL OADR

cc: Atch

SECRET

25X1

SUBJECT: Reports on Computer Security for SCI-Handling Systems

users; accountability of operating actions; and labeling of SCI information. The findings and recommendations of the Technology Panel are provided to you for your use and comment (See Attachment 3). When these "action-oriented" recommendations are arrayed against the identified vulnerabilities of the "critical" systems and the threat against them, it will lead to a plan for significant improvement in Community COMPUSEC. I intend to pursue these recommendations, in coordination with other computer security initiatives, to strengthen the protection of SCI material in computer-based systems.

25X1

5. These documents are also being provided to the appropriate officials with responsibilities assigned by NSDD/145.

25X1

William J. Casey

Attachments:

25X1

1)
2) Computer Security Technology Assessment Report
3) Uniform SAFEGUARDS for Protection of "Critical Systems" Processing Intelligence Information

25X1

SUBJECT: Reports on Computer Security for SCI-Handling Systems

Distribution:

Copy 1 - DCI (William J. Casey)
2 - SecDef (Caspar W. Weinberger)
3 - DDCI (John N. McMahon)
4 - EXDIR/CIA (Jim Taylor)
5 - ASD(C^{3}I) (Don Latham)
6 - D/INR (Hugh Montgomery)
7 - D/DIA (LtGen James A. Williams, USA)
8 - D/NSA (LtGen Lincoln D. Faurer, USAF)
9 - D/DNI (Rear Admiral John Butts, USN)
10 - Assistant Director, Intel. Div., FBI (Edward J. O'Malley)
11 - DOE/DAS, Intelligence (Charles Boykin)
12 - Treasury (Douglas Mulholland)
13 - Air Force, Under Secretary (Edward C. Aldridge, Jr.)
14 - Army/ACSI (LtGen William E. Odom, USA)
15 - Air Force/ACSI (MajGen James C. Pfautz, USAF)
16 - USMC/DI (BG Lloyd W. Smith, USMC)
17 - NSC (Ken deGraffenreid)
18 - National Security Advisor (Robert McFarlane)
19 - DUSD/P (Gen. Richard G. Stilwell, USA Ret.)
20 - Justice Dept (Mary C. Lawton)
21 - DOC (Irving P. Margulies)
22 - Chm/IPC/CIA (Richard Kerr)

25X1 **1 - OS/C/ISSG (w/att 2 only--3 copies)**
25X1 **1 - DIA/RSE (w/att 2 only--15 copies)**
1 - State (Lynn McNulty) w/att 2 only--2 copies)
1 - OSD (Gene Epperly) (w/att 2 only--3 copies)
25X1 **1 - SECOM (w/att 2 only--5 copies)**
25X1 **1 - s (w/att 2 only--5 copies)**

UNIFORM SAFEGUARDS FOR PROTECTION OF "CRITICAL SYSTEMS" PROCESSING INTELLIGENCE INFORMATION

December 1984

* * *

Supplement to:
"Security Policy on Intelligence Information in Automated Systems and Networks"
DCID 1/16
dated
4 January 1983

25X1

WARNING NOTICE
INTELLIGENCE SOURCES
OR METHODS INVOLVED

FOREWORD

The Deputy Director of Central Intelligence (DDCI) directed that security SAFEGUARDS be developed to reduce the vulnerabilities associated with processing information derived from sensitive methods and sources in "critical" automated systems and networks. These "critical" systems were identified by the senior members of the intelligence community and uniform assessments of the security of these systems were made using an early draft of these SAFEGUARDS. These SAFEGUARDS identify security requirements which, when satisfied, will significantly reduce the vulnerabilities identified in the assessments of the critical systems. These SAFEGUARD requirements are intended as a transitional step for the Intelligence Community to reduce security risks that are inherent in existing critical systems. The Intelligence Community will use the trusted security products and services of the DoD Computer Security Center as soon as such products and services are developed and are available to be incorporated into the Community's inventory of automated systems. These SAFEGUARDS reflect DCI requirements for reducing near term risks until trusted systems are available and therefore are intended to complement the DoD Computer Security Evaluation Criteria. The SAFEGUARDS are mandatory for all critical systems and voluntary for all other systems processing information derived from sensitive methods and sources. (U)

Table of Contents

* * * * * * *

Approved For Release 2009/06/30 : CIA-RDP89B01354R000100170030-0

IX. GLOSSARY

ACCESS. A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

AUTHENTICATION. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified.

COMPARTMENTED MODE. See Section VI.

"CRITICAL SYSTEM." For this document, a "critical system" is a computer system processing and/or storing intelligence information that has been selected by senior officials in the National Security Community.

DATAGRAM. A datagram is an internet protocol packet; the packet is made up of a header and trailer. For the purpose of this document the datagram is the equivalent "packet" of data as defined by the network being utilized.

DCI. Director of Central Intelligence.

DCID. Director of Central Intelligence Directive.

DDCI. Deputy Director of Central Intelligence.

DEDICATED MODE. See Section IV.

ESCORT. Duly designated personnel who have appropriate clearances and access approvals for the material contained in the ADP system and are sufficiently knowledgeable to understand the security implications and to control the activities and access of the individual being escorted.

ISSO. Information System Security Officer.

INTELLIGENCE INFORMATION. For purposes of this policy statement, intelligence information means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources and methods, that has been classified pursuant to Executive Order 12356 (or successor order). "Foreign intelligence" and "counterintelligence" have meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982.

LOW WATER MARK. Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the nonhierarchical categories.

MULTILEVEL MODE. See Section VII.

NFIB. National Foreign Intelligence Board.

OBJECT. A passive entity that contains or receives information. Access to an object potentially implies access to information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bytes, words, fields processors, video displays, keyboards, and clocks, printers network nodes, etc.

SBI. Special Background Investigation.

SENSITIVE COMPARTMENTED INFORMATION (SCI). All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

SENSITIVITY LABEL. A piece of information that represents the security level of an object and that describes the sensitivity (e.g. classification) of the data in the object.

SESSION. An activity for a period of time; the activity is access to a computer/network resource by a user; a period of time is bounded by session initiation (a form of logon) and session termination (a form of logoff).

SESSION SECURITY LEVEL. The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates.

STORAGE OBJECT. An object that supports both read and write accesses.

SUBJECT. An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state.

SUBJECT SECURITY LEVEL. A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level.

SYSTEM HIGH MODE. See Section V.

TRUSTED. Employing sufficient integrity measures to allow its use for processing intelligence information involving sensitive sources and methods.

USER. A user is an individual and/or processes operating on his or her behalf.